System Security Plan Review

Overview

In an effort to continuously improve the quality of their system security plans and supporting documentation, SFA has undertaken the objective of reviewing the major application and general support system security plans.

Details

The review of the CPS, MDE and SAIG security plans were conducted by comparing the contents of the National Institute of Standards and Technology (NIST) Special Publication 800-18, *System Security Plan Guidance* to that of the system security plans. Specific questions were extrapolated from NIST 800-18, inserted into a database and collated by 800-18 headings and control.

Each question extrapolated from NIST 800-18 is inserted into a treeview control with nodes being the headings from 800-18, subnodes are the controls from 800-18 and the questions extrapolated from NIST 80-18 are the leaves of the treeview. When a user expands the tree down to the NIST 800-18 guidance question (leaf), four fields are displayed:

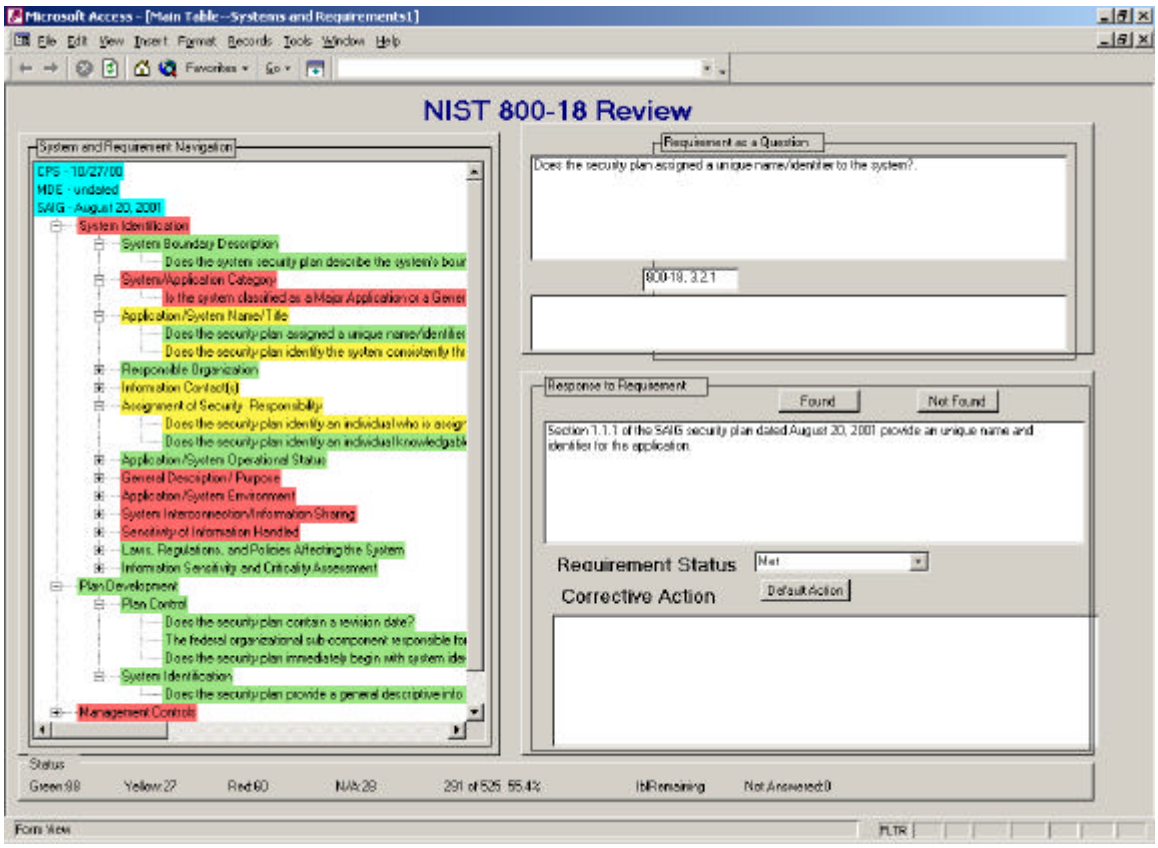
- Question,
- Status,
- Assessment, and
- Corrective Action.

As the user reviews the full question and enters comments into the assessment and corrective action fields. The status field is comprised of four values and their corresponding background color codes:

- Not met ➔ Red,
- Partially Me ➔ Yellow,
- Met ➔ Green, and
- Not Applicable ➔ Gray.

After the user selects the status field, the treeview updates appropriately to the status high level so that if any questions under a control is classified with a status of “Not Met”, the entire control is designated as “Not Met”. By color-coding the nodes and leaves of the treeview, any residual questions not answered remain with a white background and are easily found.

Below is a screen shot of the application as a user enters information for the date of authorization of system interconnections.



General Findings

Overall, the more recent the security plan date, the more consistent with 800-18 was the security plan. The MDE security plan was not generally consistent with 800-18, however the documentation provided could easily be moved into the 800-18 format. MDE should immediately transition their "risk assessment" template into 800-18 format.

The CPS security plan was generally consistent with 800-18, however it has some superficial inaccuracies and some information was not contained in the plan that should have been included. There were 28 specific questions that the security plan failed to address or were incorrectly addressed in context. CPS should immediately address the following two items:

- Even though CPS did have a security plan, the original authorization date was from 1995 and in the six years of operation, a risk assessment was never conducted. NIST and NSA guidance mandate that a risk assessment be conducted prior to a system being authorized to operate
- CPS should also immediately begin preparing system interconnection agreements with all of the systems with which it connects.

The SIAG security plan was the plan that most closely followed the NIST 800-18 template. Details of the CPS 800-18 compliance review can be found in Appendix A for items not meeting guidance, Appendix B for items somewhat meeting guidance and Appendix C for items meeting guidance.